ATTACHMENT B

(19-SW-00143-JTM)

Property to be seized

1. All records relating to violations of 18 U.S.C. 1343, 18 U.S.C. 1349, and 18 U.S.C. 1028(A)(a)(1), those violations involving the group known to its members as The Community and/or GARRETT ENDICOTT and occurring on or after March of 2017, including:

a. Records and information relating to a conspiracy to defraud the victim identified as TH;

b. Records and information relating to the SIM Hijacking and identify theft of TH;

c. Records and information relating to the unauthorized access of the mobile phone numbers and online accounts of TH;

d. Records and information pertaining to the transfer of cryptocurrency stolen from TH;

e. Records pertaining any and all discussions concerning SIM Hijacking, account takeovers, and the theft of cryptocurrency;

f. Records and information relating to the Discord user garrett#5198 or user ID 275079871896748032; gendicott99@gmail.com; Skype user haloreachfk; any username referencing “Halo”.

g. Records and information relating to the identity or location of members of The Community that conspired to steal cryptocurrency;

h. Records and information relating to communications with Internet Protocol addresses 76.0.3.210, 97.88.169.146, 153.91.225.103, or 76.0.0.140;

2. Records and information relating to cryptocurrency wallet addresses, including any cryptographic keys, recovery seeds, or passwords, in any form-used to access those addresses through any computer programs or online exchanges;

3. Cryptocurrency wallets, wallet addresses, hardware wallets (such as Trezor or Ledger devices), private keys, wallet recovery seeds, usernames, passwords, mnemonic pins, PGP keys and 2FA devices;

4. Cryptocurrencies to include but not limited to Bitcoin, Ethereum, Ripple (XRP), Bitcoin Cash, Litecoin, EOS, Binance Coin, Stellar, Cardano, Monero, Zcash, Dash, Dogecoin, and Verge. Seizure of cryptocurrency will be effectuated by (1) identifying wallets and their cryptographic keys through the seizure of information described herein, and (2) transferring the virtual currency to a government-controlled wallet.

5. Computers, cell phones, mobile computing devices, or storage media that may have been used as a means to commit the violations described above or contain the information described above**.**

6. For any computer, cell phone, mobile computing device, or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

7. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the reviewing agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.